Cybersecurity experts outline challenges associated with FirstNet, other public-safety communications

Urgent Communications By Donny Jackson

May 19, 2016

FirstNet plans to provide state-of-the-art cybersecurity by employing innovative methods that offerors are expected to propose in the request-for-proposals (RFP) process, but the entire public-safety community needs to take action to help ensure that subscriber agencies are not negatively impacted by cyberthreats, according to a panel of cybersecurity experts.

FirstNet's cybersecurity goal—outlined in the RFP, which calls for proposals to be submitted by May 31—is "ensuring end-to-end security for the FirstNet network," according to Glenn Zimmerman, senior security architect for FirstNet. There

"Each of the subdomains that comprise the FirstNet network have to stand on their own and be secure," Zimmerman said during a cybersecurity panel conducted at IWCE 2016 in March. "And, when you put it all together, the holistic aggregate of those subdomains needs to be secure, as well. That means what we're looking for is designing offsets within each of those domains to counter a failure in another aspect of the overall network.

"There is never, from a planning perspective, the assumption that anything is fool-proof. The reason is that fools are actually pretty ingenious. They'll figure out a way around almost everything. That's why you have to have means and methods to counteract and mitigate those threats, capabilities and inherent weaknesses."

Patrick Flynn, Intel Security's director of homeland/national security programs, said this philosophy makes sense, noting that FirstNet is going to have a "giant target on its back" in the eyes of hacking community and "you're going to get hacked, so you better have a good sandbox."

Indeed, Intel already is seeing a notable proliferation in the occurrence in the cyberthreats launched against its own existing customers, based on its global database of cyberattacks, he said.

“Do you know how many times it receives hits in a day? 4 billion hits a day—things that are changed, things that are bad, things that are manipulated, that sort of thing,” Flynn said. “That’s the dynamic nature of the profession that we choose today in security—it’s very, very dynamic.”

Flynn applauded the FirstNet approach to cybersecurity, because cybersecurity is being integrated into the nationwide public-safety broadband network (NPSBN) from the design phase and the RFP allows enough flexibility for vendors to propose innovative approaches to address the difficult problem.

That was by design, according to Brian Kassa, FirstNet’s director of technology planning and development.

“Engineers love to write requirements … and we could have written an RFP that had 10,000 requirements,” Kassa said. “But, when you write a requirements-based acquisition, you start limiting the creativity that potential offerors could bring. So, we went with an objectives-based RFP.”

“When we start to get responses back and hopefully make an award late this year, we will fully understand what our cybersecurity solution is. But until then, it’s safe to say that Glenn and I are kind of like kids at Christmas: We know Christmas is coming, we see stuff starting to show up under the Christmas tree, and we’re kind of excited to see what may be coming shortly.”

Designing and implementing a secure network is challenging, but the task is made even more difficult by the fact that FirstNet ’s security and authentication solutions need to be easy and quick for first responders to use.

“My view and operating philosophy is that the best security is as invisible to the user as possible and requires minimal interaction on their part—it just works,” Zimmerman said, noting that technologies such as biometrics , pattern recognition and voice recognition could be leveraged in a potential solution.

Kassa said that this is one area where it is important that the larger public-safety community understands the FirstNet offering and adopts policies that integrates its cybersecurity protocols.

“At the end of the day, a public-safety agency can add security layers on top of what FirstNet does; that’s where it really comes down to policy,” Kassa said. “We may be able to provide some of the things that Glenn mentioned—biometrics and things like this—but if your agency policy says, ‘We don’t trust biometrics, and I have to use a 15-character, upper-case, lower-case password,’ and a police officer has to type that in, something has gone horribly wrong.

“Security has now potentially interfered with (1) his ability to do his job, and (2) his very life safety. You have to consider—if you are a public-safety agency that is going to be coming onto FirstNet, to really look at what we’re going to offer within the FirstNet network and see if that’s going to meet your security policy. If it doesn’t, maybe look at your security policy to ensure that the two things mesh … The whole concept is that first responders need to be able to do their job, and cybersecurity should not prevent them from doing that. But it does need to protect them.”

Zimmerman said that FirstNet plans to vet equipment on its network that could provide the greatest potential security risks. But new technologies that provide communications interfaces to the public could be more problematic, particularly sensors and other devices associated with the Internet of Things (IoT), he said.

“Security is to the Internet of Things as shame is to a politician—neither have any; there are just blatantly stupid things that happen,” Zimmerman said, citing the example of an LED light bulb from an unnamed manufacturer that connects to the Internet. “It has no lockdown whatsoever and provides a wonderful direct gateway to your internal Wi-Fi network at home.”

While commercial IoT sensors can provide valuable situational data to first responders on occasion, public safety’s most common input from citizens is through the 911 system, which is in the early stages of transitioning to next-generation 911 (NG911). This all-IP platform should integrate well with FirstNet ’s all-IP broadband system, but NG911’s ability to receive text, data, photos and video—as well as traditional voice—does create new cybersecurity concerns, Kassa said.

“As we move to next-generation 911, we can send video to a PSAP , we can send text, we can send payloads of just about anything that is multimedia in nature,” Kassa said. “So, now we have a problem where I’m getting video, and I’m getting texts. I don’t really know what’s in these files, but I know these are all great attack vectors. How many of you have opened up the wrong e-mail and had your IT department come and find you, because you infected the entire network?”

Zimmerman said that there are a variety of techniques that would allow such multimedia files to be opened and inspected for viruses and other potential cyberthreats quick enough to meet the needs of public safety. Some technologies can clean files of malicious software, but there may be a tradeoff, he said.

“The qualifier is that occasionally—because of the heinously invasive and intertwined nature of some types of attacks—by the time it cleans it [the file], it’s blank; there was nothing that was able to be preserved,” Zimmerman said.

“In those instances, the system has to be able—in real time—to make the determination that, ‘I can clean this right now, but the problem is that there will be nothing left to review. I will pass it in a protected mode, so it can be viewed in another part of the system, but it cannot communicate with any other part of the system.’ So you can pull that data, then it will immediately flush it out and log that it was a contaminated message.”

If the contaminated message contains information that is critical to the response—for instance, video of a suspect fleeing a crime scene—and ideally would be shared as quickly as possible, determining how to handle that file becomes more complicated, Kassa said. Sharing such files may help the immediate response effort, but it could compromise public-safety user devices and the larger system in the long term.

“[That] is something we’ve got to figure out as a whole community,” Kassa said. “FirstNet will be able to get that very quickly to the responder. But if it’s infected when you stick it in the pipe, it’s going to be infected at the other end of the pipe, because we don’t we don’t want to be in the situation of cleaning out the file. So, it’s something we’ve got to figure out.”

Link to Article

Link to Urgent Communications News Articles